REMARKS

Double Patenting

Claims 1-4, 12-15 and 23-26 were rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims of co-pending application 10/661,903. Applicants acknowledge that a terminal disclaimer may be filed to overcome this rejection. However, because the claims of both applications are currently pending and subject to amendment, Applicants will delay determination as to whether a filing of the terminal disclaimer is a proper course of action until an allowable set of claims has been identified.

Rejections under 35 U.S.C. §103

Claims 3, 15 and 25 were rejected under 35 U.S.C. §103 as being anticipated by Liu (U.S. Patent 2002/0154635) which incorporates the reference of Caronni et al. (U.S. Patent 6,970,941) and further in view of Shimbo et al. (U.S. Patent 6,185,680).

Upon review of the office action, it would appear that the Examiner meant to state that claims 1, 2, 4, 5, 8, 9, 11, 12, 13, 14, 23, 24 and 26 were rejected under this combination of references.

Liu:

Liu describes a method of enabling communications between a first private network and a second private network. As described in the Abstract of Liu: "...When communicating a packet from the first private network to the second private network, a computer receives a packet from a source node in the first private network. The computer then determines whether the packet is destined for the second private network. Thereafter, if the packet is destined for the second private network, the computer forwards the packet to a destination node in the second private network. When communicating a packet from the second private network to the first private network, a computer receives a packet from a source node in the second private network..."

Liu therefore describes a method and apparatus for communicating *between* private networks.

Caronni:

Caronni describes establishing a 'Supernet' which is a private network that uses components from a public-network infrastructure. At col. 4, lines 36-60 Caronni describes:

> "... A Supernet allows an organization to utilize a public-network infrastructure for its enterprise network so that the organization no longer has to maintain a private network infrastructure; instead, the organization may have the infrastructure maintained for them by one or more service providers or other organizations that specialize in such connectivity matters. As such, the burden of maintaining an enterprise network is greatly reduced. ...
>
> Supernets also provide heterogeneous addressing functionality. The Supernet uses a separate layer that isolates address names of nodes from addressing schemes and delivery schemes. The Supernet contains a modification to the IP packet format that can be used to separate network behavior from addressing. As a result of the modification, any delivery scheme may be assigned to any address, or group of addresses...."

Caronni describes the address translation scheme in more detail at column 6, lines 6-25:

> "... the system provides address translation in a transparent manner. Since the Supernet is a private network constructed from the infrastructure of another network, the Supernet has its own internal addressing scheme, separate from the addressing scheme of the underlying public network. Thus, when a packet from a Supernet node is sent to another Supernet node, it travels through the public network. To do so, the Supernet performs address translation from the internal addressing scheme to the public addressing scheme and vice versa. By separating the addressing schemes, the Supernet creates a flexible delivery scheme that is easily changeable by network software or a system administrator. ***To reduce the complexity of Supernet nodes, system-level components of the Supernet perform this translation on behalf of the individual nodes so that it is transparent to the nodes.*** Another benefit of the Supernets' addressing is that it uses an IP-based internal addressing scheme so that preexisting programs require little modification to run within a Supernet..."

The Supernet of Caronni is thus merely a virtual network layered on top of the Internet IP network. For example, as described in the Abstract of Caronni 'The virtual network uses a separate layer to create a modification to the IP packet format that is used to separate network behavior from addressing..."

Figure 4 of Caronni illustrates an embodiment of the Supernet, which includes multiple nodes 316, 318, 320 and 322 which communicate with each other via shared channels. As described at column 5, lines 7-11 of Caronni "... When communicating among themselves, the nodes 316, 381, 320 and 322 serve as end points for the communications..."

At column 12, lines 10-20, Caronni recites:

"... When encrypting the packet, the virtual source node address 642, the virtual destination node address 644, and the data may be encrypted (addressing section 660), but the source and destination real addresses 614, 616 (delivery scheme section 670) are not, so that the real addresses can be used by the public network infrastructure to send packets to the destination..."

Applicant's respectfully note that there is no mention or suggestion in Caronni of encrypting or otherwise transforming the Supernet header.

The Examiner states, at page 4 of the office action:

"... Liu/Caronni does not disclose expressly appending a gateway source address with the source address of the packet to the second portion..." but goes on to state "... Shimbo teaches appending a gateway source address with the source address of the packet to the second portion (Shimbo, column 26, line 28-36 & Caronni: Figure 2 B & Column 12, lines 11-19)... It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Shimbo within the system of Liu because (a) Liu teaches a mechanism to extend private networks onto a public infrastructure .... Caronni teaches modifying an IP packet format so that any type of delivery scheme may be assigned to any address ... and (b) Shimbo teaches providing an efficient, flexible and secured method to protect the data communication in any type of networks such as hierarchical organized or mobile computing environment by using a security gateway (Shimbo: column 3 line 39-50).

Shimbo:

Shimbo describes a packet authentication and packet encryption/decryption scheme for a security gateway suitable for a hierarchically organized network system and a mobile computing environment. For packet authentication, in addition to the end-to-end authentication at the destination side packet processing device, the link-by-link authentication at each intermediate packet processing device in the packet transfer route is used (Abstract).

Shimbo describes ata column 26 lines 28-34:

"... Then, the security gateway GA11 carries out a processing called capsulization in which a new packet is generated by regarding the entire received packet as data and attaching the address of the security gateway GA11 as a source address and the address of the security gateway GB1 as a destination address. In addition, the security gateway GA11 calculates the authentication code for the received packet by using the authentication key K, and the capsulized packet is transferred after attaching the authentication code..."

Applicants note that although Shimbo describes the use of a security gateway address, there is no mention or suggestion that the address is encrypted or otherwise transformed. Rather it would appear that the security gateway address is used to route across the backbone..

Applicant’s Argument:

It is well known that "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)...” (M.P.E.P. 2131) Applicants respectfully submit that neither Liu nor Caronni, alone or in combination teach or suggest every element of the independent claims of the present invention.

As described above, Liu describes a system and method of interfacing two different private networks. Thus, Caronni describes encrypting the virtual source and destination addresses, and appending a Supernet header and Outer IP header to communications to implement a Supernet. There is no mention or suggestion that the Supernet header is encrypted or otherwise transformed.

Shimbo describes a system wherein gateway address is used, but again there is no mention or suggestion that the gateway address is encrypted or otherwise transformed.

In contrast, the claimed invention, as amended, now clearly recites that the transformed packet of the present invention introduces a new ‘group’ header, which includes a gateway source address and group identifier. This group header is transformed, while the original header is used to forward the packet across the backbone. The advantage of such a configuration reduces the number of point to point connections in the network, and thus reduces the amount of routing information that must be stored, while preserving data as it is transferred across the internet, as described at page 10 of Applicant's specification, which recites:

'With such an arrangement, the amount of data that needs to be stored at each of the trusted ingress and egress points is limited to the number of private groups in the VPN, rather than the number of connection paths...The present invention modifies the existing concepts of where the security boundaries need to be established in order to facilitate network scalability..."

No such advantage is realized by Caronni, Liu or Shimbo, either alone or in combination.

Applicants respectfully note the contrast between Figure 4 of Caronni and Figure 3 of the specification of the present application, which clearly illustrate various sites (Site 1, Site 2, Site 3 and Site 4) which are coupled together via a provider backbone. Applicant has amended the claim to more clearly recite that the gateway source address, associated with the source site, is inserted in the transformed packet. No such structure is shown of suggested by Caronni or Liu, or Shimbo, alone or in combination.

Claims 1, 2, 4-6, 8, 9, 11-14, 23, 24 and 26:

Independent claim 1 recites the steps of "...receiving a packet including a private network address comprising a source address, a destination address and a payload ... apportioning the packet into a first portion and a second portion, wherein the first portion includes fields of the packet used for transmission of the packet according the protocol of the backbone including the private network address and the second portion includes the payload ... *appending a gateway source address associated with the source address of the packet to the second portion to generate a group header and transforming the second portion of the packet according to a group security association associated with the private network to provide a transformed portion which includes a transformed group header* ... appending the first portion of the packet to the transformed portion to provide a transformed packet; and transmitting the transformed packet to the backbone using the private network address..."

Claim 1 is therefore patentably distinct over Caronni and Liu, which neither describe or suggest 'appending a gateway source address' to the packet and transforming the group header.

Independent claim 12, as amended, is also patentably distinct from Caronni and Liu, alone or in combination, for at least the reason that neither reference suggests "...generating a second header, *the second header including a gateway source address associated with the source address in the first header, and a destination address identifying the private network...*" ... "*applying the security association to the modified packet to provide a secure packet including applying the security association to the gateway source address..*"

Independent claim 23 is also patentable over Liu and Caronni, alone or in combination, for at least the reason that neither describe nor suggest "...An apparatus at a node for transforming packets for forwarding between a plurality of members of a group communicating on a scalable private network over a backbone, each of the plurality of group members communicating with the backbone via respective gateways, wherein the backbone operates according to a protocol, the apparatus comprising ... a key table, the key table including a security association for each group that the node is a member;... transform logic comprising means for modifying packets received from a source member of the group for transfer on a private network over the backbone by_ *extracting a private network address header from a received packet, the private network address header including a source and destination address ... appending, to the received packet, a group header including a group identifier associated with the private network and a gateway address associated with a source member; applying a security association to the received packet including the group header to provide a modified packet appending the private network address header to the modified packet to provide a transformed packet, where only information in the transformed packet that enables communication over the backbone is unsecured..*"

Dependent claims 4, 6-11, 15 and 26 are allowable for at least the reason that they serve to add further patentable limitations to an allowable parent claims, and it is therefore requested that the rejection of these claims be withdrawn.

In addition to the fact that the claims depend upon patentable independent claims, there are several limitations in the claims which further distinguish over Liu, Caronni and Shimbo.

For example, with regard to claim 6, although the Examiner states that 'a selected group address and group type can be used for any type of delivery scheme', it is respectfully submitted that the references *fail to teach the limitations of the claims as recited.* Thus, no mention is found or suggested in Liu, Caronni or Shimbo alone or in combination of 'and wherein the group header comprise a group type, the gateway source address, a group address and a and wherein the step of generating a group header *includes the step of copying the type of the first header to the group type...*' as recited in claim 6 and it is therefore respectfully requested that for this additional reason the rejection be withdrawn.

Rejections under 35 U.S.C. §103(a)

Claims 3, 15 and 25:

Claims 3, 15 and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Liu in view of Shimbo and further in view of Alkhatib et al. (U.S. Patent 2003/0233454). Applicant notes that claims 3 and 25 have been cancelled, and therefore will only address the rejection of claim 15.

Alkhatib:

Alkhatib describes, in the abstract:

"...A system is disclosed for establishing a public identity for an entity on a private network. In one embodiment, a first entity can initiate a request to create a binding of a public address to a private address for itself. The existence of this public address for the first entity can be made known so that other entities can use the public address to communicate with the first entity. The present invention allows entities outside of a private network to initiate communication with an entity inside a private network..."

The Examiner states, at page 11 of the office action:

> "... Liu does not disclose expressly an edge device is disposed between a first member of a private network and the backbone and wherein the step of transforming is performed at the edge device... Alkhatib teaches an edge device is disposed between the first member of the private network and the backbone, and wherein the step of transforming is performed at the edge device ...
>
> It would have been obvious to a person of ordinary skill in the art .... to combine the teaching of Alkhatib within the sytem of Liu because (a) Liu teaches a mechanism to extend private networks into a public infrastructure ... and (b) Alkhatib teaches providing a method to create a binding between public addresses when communicating over a private network..."

The Proposed Modification renders the prior art unsatisfactory for its intended purpose

In combining Caronni/Liu with Alkhatib, the Examiner is ignoring the desire of Caronni to develop a Supernet, which is layered over the virtual addresses to separate network behavior from addressing. For at least the reason that the combination would frustrate the desired goals of Caronni, it is requested that the rejection be withdrawn.

Combination neither describes nor suggests the limitations of the claims

However, assuming that one would be motivated to combine the teachings of Alkhatib with Caronni/Liu and Shimbo the combination would still neither describe or suggest the limitations of the claims. As discussed above, Caronni/Liu/Shimbo fails to describe the steps of generating a group header which includes a gateway address and is transformed for forwarding over the backbone, while retaining a portion of the addressing information for routing across the backbone. Alkhatib does nothing to overcome the inadequacies of the Caronni/Liu references. For this additional reason, it is requested that the rejection of claims 15 be withdrawn.

Claim 7:

Claim 7 was rejected under 35 U.S.C. §103(a) as being unpatentable over Liu (2002/0154635) which incorporates Caronni in view of Shimbo.

Claim 7 recites the steps of "...wherein the first header further includes a length, the group header further includes a group length, and wherein the method includes the steps of copying the length to the group length..."

The Examiner states, with regard to claim 7 "... Examiner notes any of the standard protocol format obviously conforms to standard T/L/V fields ... as a complete layout of a protocol specification..." The Examiner appears to be ignoring the limitations of the claims, and has failed to show first why Caronni/Liu/Shimbo would be motivated to add *an additional* length field and copy length fields from one header to another. For at least the reason that the Examiner's rejection does not satisfy the prima facie requirements for an obviousness rejection it is requested that the rejection be withdrawn.

Claim 10:

Claim 10 was rejected under 35 U.S.C. §103(a) as being unpatentable over Liu in view of Shimbo and further in view of Boden et al. (U.S. Patent 6,330,562).

Boden:

Boden describes, in the Abstract "...A data model for abstracting customer-defined VPN security policy information. By employing this model, a VPN node (computer system existing in a Virtual Private Network) can gather policy configuration information for itself through a GUY, or some distributed policy source, store this information in a system-defined database, and use this information to dynamically negotiate, create, delete, and maintain secure connections at the IP level with other VPN nodes...."

The Examiner relies on Boden as teaching an Internet Key Encrpytion. However, Applicants note that Boden fails to overcome the inadequacies of Liu and Shimbo as described above. For at least the reason that the combination of references fails to describe or suggest every limitation of the claims, it is requested that the rejection be withdrawn.

Conclusion:

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney at the number listed below so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

September 20, 2007
Date

/Lindsay G. McGuinness/
Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park
Acton, MA 01720
(978) 264-6664

Docket No. 120-306
Dd: 8/6/2007